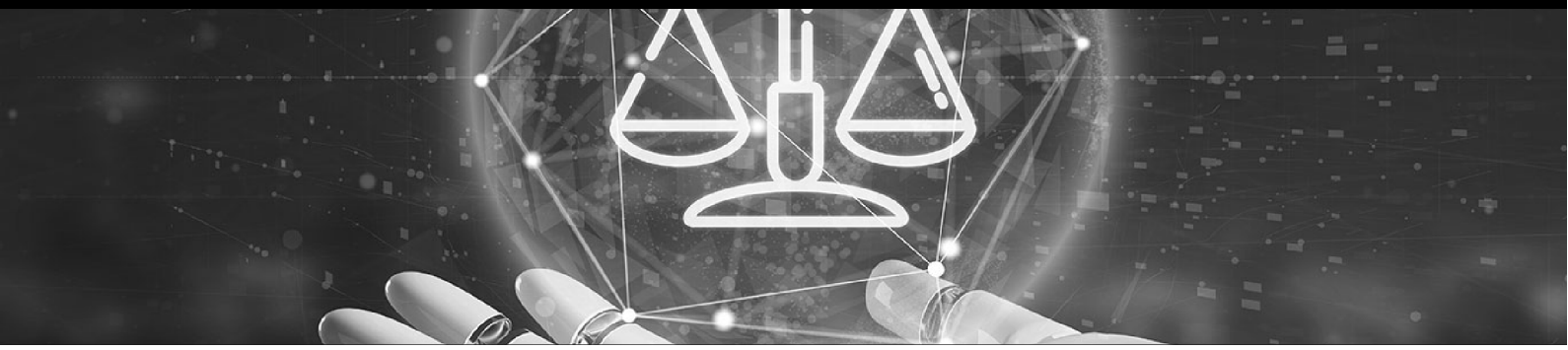
WERKSMANS
ATTORNEYS



INVESTMENT FUNDS | REGULATORY

Back to the Future: What data protection developments were there in 2024, and what lessons should SA businesses take into 2025 and beyond?

13 February 2025 *11 min read*

2024 was a big year for data protection in South Africa. The Information Regulator issued various enforcement notices and published draft regulations and guidance notes. There were also sector-specific developments in the financial services, payments, and healthcare spaces. We also saw movement in relation to AI and direct marketing.

This article examines these key developments and asks: what lessons should SA businesses take going into 2025? We discuss the various regulatory developments and consider the Information Regulator's 2024 enforcement notices, including our key take-aways for each.

Direct marketing: a spam-free 2025?

On the on hand, direct marketing is a vital business tool; on the other hand, unwanted electronic communications infringe on a person's privacy and peace of mind. The Information Regulator ("**IR**") has indicated that it has received an enormous amount of complaints relating to direct marketing.

This sets the scene for two developments in 2025:

POPIA: draft guidance note on direct marketing

The Protection of Personal Information Act No 4 of 2013 ("**POPIA**") prohibits business from conducting direct marketing by 'electronic communication' unless the person who they are marketing to (i) is their customer; or (ii) has consented.

The generally accepted interpretation was that POPIA's direct marketing provisions apply to electronic communications like email, text message, and telephone calls by automated machine, but that it does not apply to voice calls. The IR in 2024 firmly rejected this view, asserting that voice calls are also 'electronic communication'.

The IR seeks to address direct marketing in a guidance note, and a draft was published for public comment on 3 December 2024. The document includes guidance on, amongst others, what constitutes electronic communication; and how to lawfully conduct direct marketing by (i) electronic communication; and (ii) other means, like post or in person.

CPA: draft regulations

The Department of Trade Industry and Competition has proposed amendments to the regulations to the Consumer Protection Act No 68 of 2008 ("**CPA**"). The proposed amendments strengthen existing opt-out mechanisms, enhance consumers' ability to block unwanted marketing communications, and tightens rules for direct marketers' use of the opt-out registry. The mechanics of how some of the proposed amendments will work is not clear from the draft.

Public comment for the amendments closed on 15 January 2025.

It seems unlikely that we will see the amendments to the CPA regulations published this year. We're hopeful that, although controversial, the IR's guidance note is at least published in final form. This will give organisations and consumers a clearer understanding of their respective rights and obligations; as well as how the IR is going to enforce POPIA's direct marketing provisions.

Health information: critical care required

POPIA permits specific types of organisations to process health or sex life ("**health information**"), subject to its requirements. For example, medical professionals and healthcare institutions may process health information where required for a patient's treatment. Insurance companies and medical schemes may process health data relating to their specific purposes.

Nevertheless, the lawful processing of health information under POPIA is less than clear and requires more detailed guidance.

Enter the IR, who published draft regulations on processing health information under POPIA. The draft regulations apply to, amongst others, employers, insurance companies, medical aid schemes, medical scheme administrators, and pension funds. The draft regulations are onerous, for example, requiring certain organisations like insurers and medical aids to obtain consent from data subjects to process health information. The draft also contains additional rules regarding legitimate interests, cross border transfers, record retention, and destruction of health information.

Once published, these regulations will be legally binding. The current draft has been subject to criticism from industry stakeholders, and it seems unlikely that we will see these regulations published in their current form.

Cybersecurity Takes Centre Stage in the Financial Sector

The last few years have seen an increase in the frequency, severity, and sophistication of cyberattacks that target financial institutions. Financial institutions need to remain adaptive to the risks posed by cyber-attacks to withstand them, so-called 'cyber resilience'. Accordingly, it is no surprise that financial sector regulators have published rules on how institutions operating in the national payment system and the financial sector must bolster their cybersecurity and cyber-resilience.

National Payment System

The South African Reserve published a directive mandating comprehensive cybersecurity frameworks for payment institutions and operators. These frameworks must align with international best practices, integrate with operational risk management, and establish clear protocols for risk mitigation and information sharing. The directive became effective on 17 August 2024.

Financial institutions

The Financial Sector Conduct Authority and the Prudential Authority published a joint standard on cyber security and cyber resilience which applies to various categories of financial institutions. The standard, amongst others, requires financial institutions to notify the responsible authority upon the occurrence of a material cyber incident or information security compromise.

The standard will commence on 1 June 2025. Thereafter, financial institutions will be afforded a 12-month grace period within which to comply.

The directive and standard are a necessary and welcome step in the protection of financial and payments institutions and their data.

AI Regulation: Mapping Tomorrow's Rules

In August 2024, the Department of Communications and Digital Development published a draft National AI Policy Framework for public consultation. The framework is intended to serve as the basis for the National AI Policy that will guide AI regulation. As it relates to data protection, the framework envisions the safeguarding of personal information through various means, including bolstering of existing data protection regulations.

The document is likely to undergo further amendment based on the comments received from the public.

IR enforcement decoded

While new regulations shape tomorrow's compliance landscape, today's lessons come from yesterday's enforcement. The IR issued seven enforcement notices in 2024 relating to POPIA non-compliance, each revealing critical compliance insights. We discuss the enforcement notices in the following table:

Responsible Party	Facts	Key Takeaways
Department of Basic Education ("**DBE**")	The IR issued an enforcement notice against the DBE stating that it cannot publish the matric results in newspapers as this violated POPIA: the DBE did not have consent or an alternative lawful basis for processing (see next column). The DBE announced that it would publish the results anyway, and the IR subsequently issued an infringement notice fining the DBE fining it R5 million for non-compliance. The IR filed an urgent interdict against the DBE trying to prevent it from publishing in newspapers. The matter was struck off the roll for lack of urgency. The fine is presently suspended pending a review application which the DBE filed with the High Court.	Despite the IR's failure in the court process, this enforcement notice indicates how the IR interprets the requirement in POPIA that a party must have a lawful basis to process personal information. When justifying processing on the basis that – • it is necessary for performance in terms of a contract – a fact-based assessment must be made to determine whether the processing is in fact necessary for the objective pursued by the contract; • there is a legal obligation to process the personal information – such obligation must be required. In this case, the IR found the policy documents and regulations cited by the DBE insufficient evidence of any legal obligation; • the processing is in the legitimate interests of the organisation – the organisation's interest must not be confused with the prosper for processing. The IR stated that the DEB failed to evidence which of its' interests were being advanced by the publication and on what bases. This enforcement notice also indicates the IR's position that consent is not the only lawful basis for processing – a mistake organisations often make. Consent is not necessary where another lawful basis exists.
Dis-Chem	In April 2022, one of Dis-Chem's operators suffered a cyber incident which led to an unauthorised person accessing the personal information of over 3.5 million Dis-Chem customers. The IR found that DisChem failed, amongst others, to – • identity the risk of using a weak password; • put in place measures to detect a breach; • have an operator agreement in place with its service provider; • have other adequate security	This decision reinforces the imperative of ensuring proper security controls, which includes – • conducting a personal information impact assessment to assess POPIA compliance; • having operator agreements in place with all operators; and • having a compliance framework which includes reporting obligations. Dischem was ordered to conduct / put in place the items mentioned in the previous paragraph. It was also required to put in place an incident response plan which includes the incident response steps and makes provisions for all aspects of POPIA and the Cyber Crimes Act, 2020.

Responsible Party	Facts	Key Takeaways
	measures in place; and • notify data subjects of a data breach as soon as reasonably possible.	The IR also stated that an organisation must comply with all industry standards that apply to it. In this case, Dis-Chem was required to implement the Payment Card Industry Data Security Standards.
Independent Electoral Commission ("**IEC**")	The IEC suffered a security compromise in March 2024 which resulted in the disclosure – and subsequent sharing on social media – of candidate nomination lists of several political parties. The IEC said that the security compromise was as a result of an IEC officer distributing the candidate nomination lists without the authorisation to do so. The IEC failed to comply with the orders of the enforcement notice and was subsequently issued an infringement notice of R100,000.	Access control measures within a responsible party are important not only in relation to preventing external malicious actors but also from ensuring that, internally, only persons that are authorised to access and process personal information may do so. Organisations are well-minded to ensure that only personnel who need to know information to do their work, have access to that information. The more sensitive data is (and greater risk there is for data subjects if the information is disclosed), the stricter the access control processes should be.
FT Rams Consulting ("**Rams**")	The IR investigated Rams after a data subject complaint and found that it breached POPIA's provisions relating to unsolicited direct marketing by electronic means by – • not obtaining consent from the data subject nor using the prescribe form; and • failing to include contact details in the emails to the data subjects informing them of who to email to opt-out of direct marketing. Additionally, the IR found that Rams did not collect the personal information directly from data subjects; nor take reasonable steps to provide notice to data subjects.	This enforcement notice provides guidance for organisations on how to comply with their direct marketing obligations, including that: • Organisations must use the form prescribed by the IR for obtaining the data subject's consent for direct marketing purposes. Specifically, the consent must allow for the data subject to indicate how they would like to receive direct marketing communication. • A consent for direct marketing can be included in the same initial communication setting out the organisation's services or products, provided that, should the data subject "opt-out" or "unsubscribe", the organisation must immediately stop sending the data subject direct marketing communication.
WhatsApp	The IR found that WhatsApp had adopted different terms of services and privacy policies for its European and South African markets.	This decision is important as it indicates that IR's stance that where the EU GDPR and POPIA apply to your organisation, it expects you to provide the same safeguards under both laws and not weaker safeguards for POPIA.
Drs Mauff AC & Partners t/a Lancet Laboratories ("**Lancet Labs**")	Following an influx of security compromise notifications from Lancet Labs, the IR found that it breached POPIA's security safeguard provisions.	The decision shows that merely adopting privacy and retention policies is not enough to demonstrate compliance with POPIA: these policies must be fully implemented and consistent with POPIA. In relation to records retention: personal information may only be kept for as long as is necessary to achieve the purpose it was collected for and not indefinitely. The IR referred to the security controls of implementing a

Responsible Party	Facts	Key Takeaways
		information security policy and distributing it to employees; and having qualified information security personnel.
Blouberg Municipality ("**Municipality**")	A former employee complained that the personal information supplied to the Municipality as part of a declaration of interest program had been made publicly accessible on the Municipality's website. The IR ordered the removal of the complainant's personal information from the Municipality's website and found that the Municipality did not have a compliant privacy policy and PAIA manual on its website.	The enforcement notice evidences that personal information, including information relating to employees, should only be used for the purpose which it was collected for. The decision also shows the importance of ensuring that an organisation's PAIA manual and privacy notice comply with the applicable laws.

Conclusion: the way forward

The message for 2025 is clear: organisations face an increasingly layered compliance landscape where general POPIA principles intersect with sector-specific requirements. Success requires a dual focus: maintaining robust general compliance while adapting to emerging industry obligations. As enforcement actions demonstrate, regulators are ready to act – making proactive compliance more critical than ever.

Armand Swart

Director

View Profile

Hlonelwa Lutuli

Associate

View Profile